



Data recovery specialists keep finding new ways to trace criminals using the electronic clues they leave behind. **Jon Thompson** explores the frontiers of computer forensics

According to forensic scientists, unless you physically destroy a hard disk the data it contains is probably still retrievable, even after reformatting or overwriting. Has this left criminals with nowhere to hide? To find out, *Computer Shopper* talked to some of the UK companies the police turn to when searching for computerised clues.

Computer forensics used to be the stuff of science fiction, and subject to much speculation and rumour. But now, in a world dependent on digital communication, this field has become as important as other forms of forensic science, and in some cases it's the deciding factor in securing a conviction.

FARE'S FAIR

Last year, police asked UK-based data recovery and forensics company Vagon International to examine the computerised booking system used by a taxi firm where two drivers had been accused of the serious assault of a passenger. What began as a minor disagreement over a fare turned to violent revenge when the pair teamed up and sought out their victim.

As is common today, the taxi firm the two men worked for had a computerised booking system with data terminals in every cab, over which information flowed about bookings and the driver's progress. The accused claimed that the log maintained by the system would show that they were nowhere near the scene of the

crime. An initial police investigation confirmed the drivers' alibis, but they smelt a rat.

The police decided to call in Vagon to examine the booking system's database. Vagon made a specially prepared clone of the system's disk and started looking for clues on the working copy. It soon became clear that the accused pair had convinced a third man with access to the system to change their work logs to show them as being elsewhere when the assault took place. This evidence of tampering prompted the police to examine records of the mobile phones owned by the two men. When confronted with this and other evidence, they decided to plead guilty.

Increasingly, criminals are going to have to learn that if any form of computer is involved, there's likely to be a digital fingerprint just waiting for detection. A range of sophisticated techniques can recover data after what seems like its total destruction, so deleting or changing those fingerprints won't work, either.

FORGOTTEN, BUT NOT GONE

Operating systems unwittingly aid in data recovery operations. Many people don't realise that when a user deletes a file, it remains on disk. In Microsoft Windows, for instance, even after emptying the Recycle Bin, nothing much actually happens. The space that the deleted files occupied is simply marked for reuse. The operating system doesn't blank the original content. So on a large hard disk with lots of free

space, the deleted data is potentially available for reconstruction into its original files for a very long time.

According to Neil Barrett, visiting professor of computer criminology at Cranfield University in Bedfordshire, there's more to this than just being able to reverse hasty deletions at will. "You can get not just the files but the underlying structure of the disk too," Barrett said. But what would this actually give you? "It might be part of a web browser cookie showing that someone has visited a particular site, for instance," he said.

Recovering deleted files is bread-and-butter stuff to the average data recovery firm, but not



▲ Clean environments, such as this one at Norway-based IBAS, ensure that there is no loss or corruption of forensic evidence



▲ Machines such as this Guzik V2002 Spinstand tester can read between the lines when it comes to data forensics

for the average police force. Though not widely reported, it's common for forces to call on such companies to handle the technological aspects of high-profile investigations. The firms themselves are understandably discreet when it comes to naming names; see the 'Data recovery in action' box opposite. All evidence needs special care to preserve it for trial, and computer-based evidence has unique requirements. Data recovery companies, with their clean room environments, are ideal for ensuring that digital evidence remains pristine. As well as working with the police, defence teams are increasingly calling upon their services, too. Sometimes, this simply ensures that there's a case to answer.

For example, local authority watchdog The Standards Board for England called in Dataclinic Hard Disc Data Recovery Services in 2002 to examine the PC of a Stratford-upon-Avon councillor accused by IT staff of storing indecent images of children at work. Theoretically, there might have been an innocent explanation, such as a virus or a deliberate attempt to disgrace the accused man. But it soon became apparent that neither of these possibilities was the right one.

The councillor in question, Conservative Christopher Pilkington, resigned in August 2002 over the affair. He subsequently received a police caution and an entry on the sex offenders register for five years. The Standards Board for England also found Pilkington guilty of

breaching the councillors' code of conduct and banned him from running for public office for five years in January 2004.

In some circles, there's a common belief that simply using a specialist program to overwrite incriminating files with new information is enough to destroy all traces of them forever. But new and experimental techniques are making that process ever more difficult.

A HAIR'S BREADTH

By exploiting how disks work, computer scientists have discovered that they can sometimes read back overwritten data. Such techniques are becoming increasingly important in the crime fighter's arsenal.

One reason why overwritten data is sometimes still accessible lies in the tiny inaccuracies, called misregistrations, inherent in the process of moving a drive's read/write heads. The tracks on a modern disk are too narrow to align the heads perfectly every time, as each track is about one-tenth of the width of a human hair, so a sliver of old data sometimes remains alongside the new. Not being sensitive enough, the read heads in a commercial disk don't detect and are confused by this old data. But heads fitted to a machine called a spinstand tester can sometimes differentiate between newly recorded data and old slivers with ease. These machines are normally used by disk manufacturers to test the accuracy of their production process.

One example of such a machine is the Spinstand V2002, made by Guzik Technical Enterprises of Mountain View, California. The tracks on a modern disk are about 400 nanometres wide. Using tiny piezoelectric motors, the V2002 can position its heads at any point on the surface of the disk with an accuracy of 0.3 nanometres. By searching carefully, tiny slivers of old data can become visible.

This is a painstaking technique, made necessary by the severity of the crimes to which it's applied. "We have recovered names, telephone numbers and credit card details from a computer belonging to a suspected Irish

terrorist using this technique," said Vagon's Gordon Steveson.

Magnetic tapes are widely regarded as being even easier to read because their misregistrations are far larger, so overwriting backup tapes is no protection from the computer forensics lab. As the density of data increases and track widths decrease, this technique will become harder to use. Luckily, the hardware controllers used in modern disks hold the key to a second technique that could make it pointless to attempt data deletion.

LOOK, LIST, LEARN

Normal wear and tear such as knocking, dropping or moving a running computer causes a small percentage of disk sectors to become corrupt. To avoid losing the content stored on these areas, modern controllers automatically re-map their content to empty parts of the disk and mark the offending sectors as unusable. To do this they maintain two lists, called the plist and glist.

The plist, short for primary list, is the list of bad sectors uncovered when the manufacturer tested the disk before shipping. The drive controller will not attempt to use any of these for storing data, knowing them to be bad. Glist data refers to the grown defect list of bad sectors. This is the growing list of sectors that the drive marks as suspect during its lifetime. When a sector enters this list, the drive copies the data it contained to an empty sector elsewhere on the disk. It's this safety mechanism that can confound those wishing to destroy data.

The reason is that with the data safe, there's no need to inform the operating system and no need to overwrite potentially corrupt sectors. The drive just doesn't use them again. When instructed to do so, however, the controller will read these, yielding their original content if the sectors are not too corrupt. Deleting re-mapped files at operating system level does no good, because it doesn't know about this re-mapping activity. Someone with something to hide would have to re-program the disk controller to overwrite the glist sectors physically.

Estimates vary, but according to some sources up to 0.5 per cent of a notebook disk drive could appear on its glist. This may sound insignificant, until you realise that this actually represents 50MB for every 10GB.

GHOST HUNTING

Inevitably, there are times when none of the techniques explored so far will work. However, one researcher claims that, in future, the ghost of the data will still be there to find. In 1997, Dr Peter Gutmann of the department of computer science at the University of Auckland in New Zealand presented a paper to the Sixth USENIX Security Symposium. In it, he claimed that because magnetic media record and read magnetic polarities and pay no attention to the strength of that magnetisation, individual bits could contain the remnants of previous content. The thinking behind this claim is simple, but at the time many dismissed it as being too difficult to achieve with any degree of efficiency.

The theory is as follows: suppose three patches of magnetism, representing three binary ones, appear consecutively on a disk. If one of them is more strongly magnetised in the direction that represents one than the other bits, it must previously have been a one as well. If it is

CLEAN SWEEP: WIPING OLD DATA FROM PCs

How much care should you take to wipe old data from computers before selling them at car boot sales or on eBay, or giving them to charities? One company, Disklabs, decided to find out. It analysed 100 hard disks and 50 memory cards bought second hand. The results will make anyone who is considering selling old kit think twice.

"We thought it would be interesting to find out how many memory devices that we purchased we'd actually recover data from," said Simon Steggle of Tamworth-based Disklabs. The company restricted itself to techniques open to the average computer fraudster, including plugging memory cards into computers to read their content and inspecting the Recycle Bin and temporary internet files directory on hard disks. Some units contained a wide range of personal information, including passwords and credit card details. "Had we put our minds to it, we could have potentially stolen some of these people's identities," warned Steggle.

In a paper he wrote with Dr Christine Finn, Sellam Ismail, founder of the Vintage Computer Festival, said that information left in files on an Apple Mac II Classic bought locally would allow anyone to steal the previous owner's identity. "On the hard drive, I found personal letters, CVs, job applications, financial records such as bank balances and other holdings, digital photos, and email. Had I been a psychopath, I could have used the data [on the computer] to reign information terror on my neighbours."

When selling your PC, you should make sure you thoroughly clean it of all personal data. The best way to do this is to reformat the hard disk and reinstall the operating system. However, if that's beyond your means or ability, make sure you have cleared out all files that might potentially give away your details. Most are obvious, but some aren't. In next month's *Shopper* we'll show you how to delete your internet browsing history files.

CASE STUDY: DATA RECOVERY IN ACTION

Computer Shopper talked to Simon Steggles, director of Tamworth-based Disklabs, to find out more about the work of forensic data recovery companies.

Disklabs handles the digital evidence requirements for some very high-profile police investigations. One example is the case of Jodi Jones, the teenager hacked to death in woods in Dalkeith, near Edinburgh, in 2003.

Steggles said: "We some did work on the Jodi Jones case, where we examined both the suspect's and the victim's phones." A court in Edinburgh subsequently convicted the 14-year-old's boyfriend, Luke Mitchell, of her murder. "The police have to be careful when examining a mobile phone for evidence," said Steggles. "If it is turned on normally, newly transmitted text messages, for instance, could destroy those messages already on the handset." To ensure that the original material is never at risk, Disklabs carries out forensic work on copies of original data, and mobile phone SIM cards are no exception. Data forensics companies use machines for cloning the tiny cards as well as reading their content.

Though their work doesn't often make the headlines in the same way as the crimes they help to investigate, the cases that police call in computer forensics firms to help with are no less harrowing for their lack of public profile. "We have done work for international motor racing teams, government departments, covered subjects such as corporate espionage, rape cases, murder cases, internet child abuse, and many others," said Steggles.

"Retrieving data from two notebooks and a desktop computer that were water-damaged and dirty from the effects of Hurricane Katrina in the US last year was an unusual event," he continued. "Recovering data from fire-damaged hard drives was also a bit unusual, although we are seeing them more and more." Which means that throwing an incriminating hard disk into a lake or on a bonfire might not be enough to get rid of its content.



▲ The fire suffered by this hard disk controller was so hot that one chip has fallen off and the solder holding the chip on the left has melted and allowed it to shift position. Yet not only did the drive survive the fire but it also had 100 per cent of its data recovered



▲ Careful cleaning and advanced techniques can still recover data stored on seemingly ruined disks

DAMAGED HARD DISK IMAGES COURTESY OF: DANIEL JARMISHAW AT WWW.FUJI-FORUM.CO.UK



A bad translation can have embarrassing consequences.

Systran Translator Preferred 5 : The most advanced translation software of its generation.

Systran Translator Preferred 5 uses sophisticated technology that guarantees you a true translation of the word and meaning to avoid embarrassing situations as these. With seamless integration with Microsoft Office and Internet Explorer, Systran Translator is the only translation product to have on your desktop.



NUANCE.CO.UK/SYSTRAN

Available at

amazon.co.uk

ebuyer.com

Insight

MISCO

© Copyright 2005
Nuance Communications, Inc.
All rights reserved.

Nuance and the Nuance logo are trademarks and/or registered trademarks of Nuance Communications, Inc. and/or its affiliates in the United States and/or other countries. Systran and the Systran logo are trademarks or registered trademarks of Systran. All other trademarks are the properties of their respective owners.

NUANCE
ScanSoft Imaging Solutions



▲ Magnetic force microscopes such as this one operated by the Institute of Physics at Taiwan's Academia Sinica might soon be bringing back data from the dead

less polarised than average it must have previously been a zero, as represented by the opposite polarity.

Gutmann theorised that because a scanning probe microscope (SPM) can accurately read magnetic field strengths down to a molecular level, and because many commercial SPMs have physical mounting points called vacuum chucks, they should be capable of taking a disk platter for examination. "If commercially available SPMs are considered too expensive, it is possible to build a reasonably capable SPM for about \$1,400 (around £800) using a PC as a controller," Guttmann said. But it was another claim made in Guttmann's paper that caused the most controversy.

According to Guttmann, "even for a relatively inexperienced user, the time to start getting images of the data on a drive platter is about five minutes. To start getting useful images of a particular track requires more than a passing knowledge of disk formats, but these are well documented, and once the correct location on the platter is found, a single image would take two to 10 minutes depending on the skill of the operator and the resolution required."

Many openly scoffed at Guttmann's claims, including Daniel Freeberg of the US-based National Bureau of Economic Research. "A hour on the web failed to come up with a single laboratory claiming it had an ability to read overwritten data," he claimed in response to Guttmann's ideas. But times are changing, and one researcher in particular might be about to prove Guttmann right.

FIELDS OF DREAMS

Associate professor Romel Gomez, of the department of electrical and computer engineering at the University of Maryland, claims to be able to read the original content of a disk or tape completely overwritten by new content. He does this using a sensitive device called a magnetic force microscope. This measures the polarisation of groups of atoms arranged previously by a magnetic field. The more highly magnetised, the stronger the magnetising field must have been. But Gomez has discovered that the strength of polarity could be due to two successive magnetisations, just as Guttmann predicted in his 1997 paper.



▲ You can burn, bury or drop a hard disk from a building, but the data is still recoverable

Gomez claims to have read back the original data from a disk deliberately overwritten first. "This means it is not completely safe to reformat your hard disk," he warned. He cautioned about how slow the process is at present. "Extracting one kilobyte of data per hour is optimistic." It's early days and the technique is experimental, but with specialist spinstand testers already being used routinely in forensic clean rooms it might be just a matter of time before this technique is more widely used too. Soon, it seems, there'll be nowhere for data to hide and no way to delete it for good.

The intelligent criminal might think that all he has to do is smash or burn the disk or other device containing evidence that might put him behind bars. However, this could simply play into the hands of the computer forensics experts. After all, they still make most of their money recovering data from disks that have been through far worse than a bonfire. Gomez's work may mean that, in future, not even using a big magnet to wipe individual disk platters will enable someone to truly destroy magnetic data while its ghost still remains. ☐

NEXT MONTH IN COMPUTER SHOPPER

- Notebooks
- Quiet PC Components
- Digital Cameras
- MP3 Players
- Network Storage
- Anti-virus Software
- Beginner's Guide to Programming VB .NET
- Keyloggers Exposed

On sale at all good
newsagents from
20th April 2006